

**AFFIDAVIT OF JASON J. DEFREITAS IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Jason J. DeFreitas, a Special Agent with Homeland Security Investigations, being duly sworn, depose and state as follows:

1. I am a Special Agent with the Department of Homeland Security (DHS) United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI) assigned to the Boston Field Office and have been employed by HSI since 2006. I am currently assigned to the Cyber Group. Prior to my assignment to the Boston Field Office, I was assigned to the HSI Los Angeles Field Office, where I served as a member of the Intellectual Property Rights Group. In connection with my official duties, I have investigated and assisted other agents in investigating cases involving a wide variety of criminal violations including, but not limited to, fraud, intellectual property rights, cultural property theft, and child pornography. Prior to my employment with ICE HSI, I served as a United States Customs and Border Protection (CBP) officer at the Los Angeles International Airport for approximately four years. My duties included the interception and examination of individuals and merchandise for violations of United States laws.
2. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure to search the residence located at [REDACTED], Acushnet, Massachusetts 02743 (the "SUBJECT PREMISES"), as more fully described in Attachment A, which is incorporated herein by reference.
3. As described herein, there is probable cause to believe that the SUBJECT PREMISES contains contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A (possession and distribution of child pornography), which items are more specifically described in Attachment B, which is also incorporated herein by reference.

Exhibit A

4. The statements in this affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A (possession and distribution of child pornography) are presently located at the SUBJECT PREMISES.

STATEMENT OF PROBABLE CAUSE

5. Taunton Police Detective Randy DeMello, an HSI Task Force Officer ("TFO"), conducted an online investigation into the use of peer-to-peer¹ file sharing programs on the Internet to identify persons that distribute child pornography. In the course of that investigation, TFO DeMello was able to observe the activity of other users of particular P2P networks.
6. Beginning on or about January 26, 2019, TFO DeMello began to monitor activity on the eDonkey2000 network ("eD2k")² associated with the Internet Protocol address³

¹ Peer to Peer ("P2P") file sharing allows people using P2P software to download and share files with other P2P users using the same or compatible P2P software. P2P software is readily available on the Internet and often free to download. Internet-connected devices running P2P software form a P2P network that allows users on the network to share digital files.

² eD2k is one of many P2P networks. For a user to become part of the eD2k network, the user must first obtain eD2k client software, such as eMule or Shareaza, and install the software on a device, such as a computer. When the client software is running and the device is connected to the Internet, the user will be able to search for and download files made available by other users on the network and share files from his device with other users on the network.

³ An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if

24.91.14.54. The device connected to the Internet via this IP address will hereinafter be referred to as the "Suspect Device."

7. Specifically, on seven occasions ranging from January 26, 2019 to April 23, 2019, TFO DeMello learned that a device at IP address 24.91.14.54 was connected to the eD2k network and offered for distribution various digital files that were identified by TFO DeMello's investigative software as likely to contain child pornography. On these occasions, the Suspect Device reported that it was using eD2k client software eMule v0.50a⁴ and its client user hash as DA1149D4BE0EE8CC3FBFAABA31476F73.⁵
8. On January 26, 2019, between 2:06 PM and 2:33 PM, TFO DeMello, using a computer running law enforcement investigative eD2k software, observed that the Suspect Device was making available for download a file with the eD2K hash value

an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

⁴ When a user launches the eMule client program it will connect to the eD2K network. Once connected to the network, information about the files the user is sharing with peers on the network is provided to the network. Such information may include the file's eD2K hash value (defined below), the file's size, and the file name. While connected to the network, a user can look for a file through a search feature built into the client software. Doing so initiates a search among other users that have reported to the network that they have all or part of the files that matched the search criteria. In order for a user to obtain a certain file, the user must manually initiate a download process, typically by double-clicking the file name. Once the download process is initiated, the transfer of the selected files occurs directly between two or more users on the eD2K network.

⁵ A hash value is a unique algorithm-generated identifier comprised of letters and numbers, which is often thought of as a "digital fingerprint" for files or data sets. A "client user hash" is the hash value assigned to a specific user upon installation of the eMule client software. This user hash remains with a user as long as the eMule software is installed on a given device.

[REDACTED].⁶ Based on its hash value, this file was identified by investigative software as known child pornography. Using the law enforcement investigative eD2k software, TFO DeMello was able to download the file directly from the Suspect Device.⁷ I have viewed this video, which is described as follows:

- a. "PEDO-PTHC---ONLY THE BEST---2015---LOLITA COLLECTION-----NEW SERIES (204).avi" is a video that is approximately 7 minutes and 25 seconds in length. It depicts a prepubescent, nude female child who appears to be approximately 8-10 years old. In this video, the child's vagina and breasts are exposed. In the course of the video, the child is depicted rubbing her genitals, first with her fingers and later with an object.⁸
9. Over the course of April 6, 2019, April 8, 2019, and April 23, 2019, TFO DeMello directly downloaded a total of six videos suspected to be child pornography from the Suspect Device. One of these videos, downloaded on April 6, 2019, is described as follows:
 - a. "Pedo – 9Yo Girl In Mask Gets Creamed. Avi" is a video that is approximately 5 minutes and 4 seconds in length. It depicts a prepubescent, female child who appears to be approximately 9-10 years old. In this video, the child's vagina and breasts are exposed and she is shown being penetrated both vaginally and anally by the erect penis of an adult. The child is wearing a mask covering her face.⁹

⁶ The eDk2 network utilizes the Message Digest Algorithm Version 4 (“MD4”) hash value. It is computationally infeasible to find two different files having the same eD2k MD4 hash value; if two files have the same hash value, that means they are copies of the same file.

⁷ A law enforcement tool allows investigators to download certain files directly and entirely from a single source rather than from multiple users.

⁸ A still image from this video is available for the Court's review.

⁹ A still image from this video is available for the Court's review.

Exhibit A

10. An online query utilizing the American Registry for Internet Number (ARIN) of IP address 24.91.14.54 revealed that this IP address is registered to Comcast Cable Communications, LLC ("Comcast"). As a result of this information, on June 6, 2019, HSI served an administrative subpoena on Comcast, directing the company to provide records and other subscriber information pertaining to that particular IP address from January 25, 2019 – April 23, 2019, the dates on which the files described above were downloaded.
11. On or about June 7, 2019, Comcast responded with records containing the following subscriber information for the IP address:

Subscriber Name:	Paul & [REDACTED] Hodson
Address:	[REDACTED], Acushnet, MA 02743-1528
Telephone number:	508-[REDACTED]
Type of Service:	High Speed Internet Service
Email User IDs:	paulhodson@[REDACTED]
Account Status:	Active
12. According to the Town of Acushnet Assessor's Database for [REDACTED] (the SUBJECT PREMISES), Paul E. Hodson II and [REDACTED] Hodson purchased the SUBJECT PREMISES on July 24, 2008.
13. Information from the Acushnet Police Department ("APD") and from the Massachusetts Registry of Motor Vehicle ("RMV") indicates that Paul Hodson II and [REDACTED] Hodson (the "Hodsons") list the SUBJECT PREMISES as their residential address. According to information from APD, the Hodsons have a minor son (YOB 2012) who lives with them at the SUBJECT PREMISES.
14. On or about June 5, 2019, members of the APD conducted surveillance of the SUBJECT PREMISES and observed two vehicles parked in close proximity to the SUBJECT PREMISES: a Honda CRV bearing MA registration [REDACTED]; and a Hyundai sedan bearing

MA registration [REDACTED]. According to records from the RMV, both vehicles are registered to Paul E. Hodson II at the SUBJECT PREMISES.

15. According to information from APD, Paul E. Hodson II is employed as a police officer by the New Bedford Police Department ("NBPD") in New Bedford, MA. Furthermore, open-source research revealed several online articles referencing a NBPD officer with the name of Paul Hodson.
16. On June 5, 2019, members of the APD, utilizing a wireless device, conducted a search of the wireless networks in the vicinity of the SUBJECT PREMISES, which revealed that all of the wireless networks observed were secured or password-protected and not open for public use but one, xfinitywifi.¹⁰ Based on this information, I believe that the user of the Suspect Device was either directly connected to the internet inside of the SUBJECT PREMISES or was privy to the password or login information to any wireless networks used to access the Internet at the SUBJECT PREMISES during the direct downloads of child pornography described above.

Characteristics Common to Individuals who Consume Child Pornography

17. Based on my previous investigative experience related to child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who utilize web-based services to access with intent to view and possess, collect, receive, or distribute images of child pornography (*i.e.*, consumers of child pornography), as follows:
 - a. Consumers of child pornography may receive sexual gratification, stimulation, and

¹⁰ The one unlocked network was named, "xfinitywifi." I know that Xfinity is an internet service associated with Comcast. Per Comcast, these wireless networks are "hot spots" available to Comcast customers. In order to access these networks, a current customer must log in using his Comcast account information.

satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media.

- b. Consumers of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, videos, books, drawings, other visual media, and, increasingly, digital format. Individuals who have a sexual interest in children or images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.
- c. Consumers of child pornography almost always possess and maintain their child pornographic material (whether stored in hard copy or digitally) in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, videos, digital media, and other documentation of child pornography and child erotica for many years.¹¹ Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.
- d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and other digital devices through

¹¹ See *United States v. Morales-Aldahondo*, 524 F.3d 115, 117-119 (1st Cir. 2008) (3-year delay between last download and warrant application not too long, given affiant testimony that consumers of child pornography value collections and thus often retain them for a period of time, and consumers who use computers to access child pornography are likely to use computers to store their collections).

the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual “deleted” it.¹²

- e. Consumers of child pornography also may correspond with and/or meet others to share information and materials; often maintain correspondence from other child pornography consumers; conceal such correspondence as they do their sexually explicit material; and often maintain the contact information of individuals with whom they have been in contact and who share the same interests in child pornography.
 - f. Consumers of child pornography prefer not to be without access to child pornography for any prolonged time period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world.
18. Based upon all of the foregoing, I believe that a user of the Internet account at the SUBJECT PREMISES likely displays characteristics common to consumers of child pornography and submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the subject offenses will be located at the SUBJECT PREMISES.

Search and Seizure of Computer Systems and Data

19. As set forth above, probable cause exists to believe that the federal offenses described above were perpetrated through the use of computer equipment capable of accessing the

¹² See *United States v. Carroll*, 750 F.3d 700, 706 (7th Cir. 2014) (concluding that 5-year delay was not too long because “staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology”); see also *United States v. Seiver*, 692 F.3d 774 (7th Cir. 2012) (Posner, J.) (collecting cases, e.g., *United States v. Allen*, 625 F.3d 830, 843 (5th Cir. 2010); *United States v. Richardson*, 607 F.3d 357, 370-71 (4th Cir. 2010); *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010)).

Exhibit A

internet.

20. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or even years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from an old computer to a new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media – in particular, computers’ internal hard drives – contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is usually required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often

Exhibit A

maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

21. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software, or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, computer-related documentation, and storage media (“computer equipment”) be seized and subsequently processed by a qualified computer specialist in a laboratory setting, rather than in the location where it is seized. This is true because of:

- a. The volume of evidence — storage media such as hard disks, flash drives, CD-ROMs, and DVD-ROMs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine what particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements — analyzing computer hardware, computer software, or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert

Exhibit A

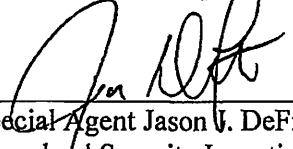
possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, password-protected, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

22. Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.
23. The SUBJECT PREMISES may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine its true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

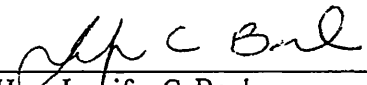
CONCLUSION

24. Based on all of the foregoing, I submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252A, as described in Attachment B, are located at the SUBJECT PREMISES, as more fully described in Attachment A.


Sworn to under the pains and penalties of perjury,


Special Agent Jason V. DeFreitas
Homeland Security Investigations

Subscribed and sworn to before me this 11th day of June, 2019.


Hon. Jennifer C. Boal
United States Magistrate Judge

I have reviewed still images from the videos referenced in Paragraphs 8 and 9 above and I find probable cause to believe that they depict minors engaged in sexually explicit conduct. The affiant shall preserve the images provided to the Court for the duration of the pendency of this matter, including any relevant audio process.


Hon. Jennifer C. Boal
United States Magistrate Judge

